La Chronique

de la Ligue des droits de l'Homme asbl

Bureau de dépôt : Bruxelles X - Périodique bimestriel | Éditeur responsable : Alexis Deswaef

22, rue du Boulet à 1000 Bruxelles | ldh@liguedh.be | www.liguedh.be | Tél. 02.209 62 80 | Fax 02.209 63 80



n°166

BELGIQUE - BELGÏE
P.P.
BRUXELLES X
1/2730

N° D'AGRÉMENT P801323

DOSSIER INTRODUCTIF
AU CYCLE D'ACTIVITES 2015

TOUT LE MONDE TOUT NU

La vie privée est-elle encore sexy ?

7/24:30! - Tout le monde tout nu
Mode d'emploi

«7/24:30!», ça veut dire quoi ?
7j/7, 24h/24: 30 articles de la Déclaration universelle des droits de l'Homme dans votre quotidien!

«7/24:30!», c'est quoi ?
Tous les ans depuis 2007, «7/24:30!» propose des activités - débats, projections, balades citoyennes, formations, expositions, performances artistiques, mises en situation - qui se répondent et se complètent. «7/24:30!» propose à chacun(e) de s'approprier davantage ses droits et de devenir acteur de sa citoyenneté. Cette huitième édition, intitulée «Tout le monde tout nu», sera consacrée au droit à la vie privée.

«7/24:30!», ça sert à quoi ?
L'objectif est d'ouvrir un espace de discussion en prenant au sérieux les questions, interrogations et craintes de tout un chacun et en mettant en lumière la dimension complexe des questions liées à diverses thématiques relatives au respect des droits humains.

«7/24:30!», ça s'adresse à qui ?
Ce cycle d'activités n'est pas une semaine d'étude entre militants spécialistes de la question. Chaque citoyen-ne pourra trouver son bonheur dans la large panoplie d'activités qui sera proposée, voire pour co-construire certaines d'entre elles avec la Ligue des droits de l'Homme.

«7/24:30!», toute l'année, près de chez vous !
«7/24:30! – Tout le monde tout nu» se déroulera de janvier à décembre 2015, dans plusieurs communes de Wallonie et de Bruxelles afin de multiplier les possibilités de vous rencontrer.

Les trois grandes journées et soirées de réflexion, de débat et de fête organisées au Centre culturel Jacques Franck, les 9, 10 et 11 octobre 2015, constituent un moment fort de ce cycle qui permettra d'aborder, de manière approfondie mais aussi ludique, plusieurs pans de cette vaste thématique qu'est le respect de la vie privée.

Et c'est quoi le programme ?
TOUT LE MONDE TOUT NU
Une initiative de la Ligue des droits de l'Homme

Durant toute l'année 2015
Un peu partout
en Fédération Wallonie-Bruxelles

Du 9 au 11 octobre 2015
Au centre culturel Jacques Franck (CCJF)
Chaussée de Waterloo, 94 à 1060 Bruxelles

Accès transports en commun (CCJF)
Tram 3, 7, 4 et 51 : Parvis de Saint-Gilles
Tram 81 : Barrière de Saint-Gilles
Métro : Station Porte de Hal
Bus 48 : Barrière de Saint-Gilles
Le centre est accessible
aux personnes à mobilité réduite.

Réservations
Durant toute l'année :
ldh@liguedh.be - 02 209 62 80
Pour les activités au CCJF
04783127463

Infos et programme (mise à jour régulière)
www.liguedh.be/72430
#toutlemondetoutnu

NOS PARTENAIRES :










Comité de rédaction
Emmanuelle Delplace et David Morelli

Ont participé à ce numéro
Helena Almeida, Jean-Pierre Borloo, Catherine Forget, Raf Jespers, François Koeune, Manuel Lambert, David Morelli, Laurie Phillips, John Pitseys, François-Xavier Standaert.

Graphisme et illustrations
Max Tiegelkamp | www.stripmax.com
Daniel Renzoni

David Morelli, coordinateur de la Commission Nouvelles Technologies LDH

Vie privée : tout le monde tout nu !

«Everyone has their own number in the system that we operate under We're moving to a situation where your lives exist as information»
Pet Shop Boys, Integral

Les goûts et les couleurs sont affaires personnelles et ne se discutent pas. Mais à l'ère de l'information et du web 2.0, ils s'exposent, circulent, se valorisent et s'échangent, parfois «à l'insu de notre plein gré», contre rémunération. Des petits bouts de nous, de ce que nous aimons, de ce que nous disons, des endroits où nous nous rendons, des biens que nous achetons, sont dispersés, sur la toile, dans nos cartes de fidélité, dans les banques de données des sociétés de marketing ou dans les enregistrements des caméras de vidéosurveillance. Au risque d'une perte de soi.

Si ces données ont déjà une valeur informationnelle et commerciale intrinsèque, l'enjeu fondamental, fondateur d'un véritable pouvoir pour les autorités et d'un avantage concurrentiel pour les entreprises privées, est de pouvoir collecter, rassembler, croiser et agréger ces informations afin de pouvoir recréer, en dehors de nous, un double informationnel, une image pointilliste de ce que nous sommes et de ce que nous pouvons potentiellement devenir. Cet avatar virtuel est-il fidèle à qui nous sommes ? Difficile de le savoir : il faudrait avoir accès à ceux qui ont construit cette version synthétique de notre personnalité afin de pouvoir la corroborer ou, a contrario, la modifier ou la faire disparaître.

Cet état de fait est-il compatible avec ce droit fondamental que constitue la vie privée ? Sous couvert d'une société de l'information qui se présente comme ouverte et transparente, n'assiste-t-on pas, en réalité, à la mise en place d'une société de la surveillance dont la vertu de transparence serait l'apanage exclusif des citoyens ?

Le 11 septembre 2001 a sans doute constitué un tournant majeur dans le rapport que l'État entretient avec la vie privée de ses citoyens. A la fois soutien et moteur de la société de l'information, le développement des technologies de l'information a permis, en appui à la lutte légitime contre le terrorisme, de multiplier la collecte et le croisement d'informations, les contrôles, les fichages, le traçage et d'accélérer, tout en la fondant, la mise en place larvée d'une société du contrôle et de la sécurité. Avec, comme conséquence, la mise en concurrence de deux libertés fondamentales – vie privée vs sécurité – et des atteintes de plus en plus nombreuses à la confidentialité, à l'anonymat.

Pourtant, le droit au respect de la vie privée est garanti dans de nombreux traités, conventions et pactes internationaux, ainsi que dans les lois ou constitutions nationales qui l'ont intégré afin d'interdire toute tentation de l'État de s'immiscer de manière abusive dans la sphère privée du citoyen. Il ne peut y être porté atteinte que dans cadre d'une mesure proportionnée et *«nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui»*.

Depuis plusieurs années, les cas de violation de ce droit se multiplient de manière alarmante. Mais elles ne sont pas le fait exclusif de l'État : les entreprises privées, les médias... et les citoyens eux-mêmes participent à la fragilisation de ce droit fondamental.

L'État tout d'abord : sous couvert de luttes, a priori légitimes, contre la criminalité, le terrorisme ou le radicalisme, les gouvernements successifs multiplient les lois liberticides. Méthodes particulières d'enquête, lois imposant le fichage généralisé, inscription d'informations privées sur la puce de la carte d'identité et mise en réseau de bases de données contenant des informations personnelles, installation massive de caméras de vidéosurveillance... Afin de renforcer la sécurité, l'État met en péril la vie privée des citoyens et participe de manière insidieuse – et peut-être pas fortuite ? – à la pérennisation d'un sentiment d'insécurité permanent. «Si tu n'as rien à cacher, pourquoi avoir peur d'être écouté ?» Réalisant l'assertion menaçante de Big Brother dans le roman visionnaire de Georges Orwell, «1984», l'État inverse la logique de la présomption d'innocence en considérant chaque citoyen comme un coupable potentiel... pour mieux le protéger. «Si tu es un État démocratique, pourquoi avoir peur de ne pas connaître notre intimité» a-t-on envie de lui rétorquer...

Si la lutte contre le terrorisme constitue l'argument massue pour justifier les mesures portant atteinte à la vie privée, la crise économique et la politique de culpabilisation des populations précaires (chômeurs, allocataires sociaux...) qu'elle entraîne facilite la mise en place de mesures de contrôle social : exigences faussement contractuelles démesurées, vérification des compteurs de gaz et d'électricité... Il s'agit au final d'empêcher le citoyen de se révolter face à l'impuissance déclarée des pouvoirs publics de procurer à la population les conditions de l'effectivité de sa dignité. Ce contrôle social s'attaque également aux sources de la contestation. Tous les prétextes avancés pour justifier une atteinte au respect de la vie privée doivent être relus à travers le prisme de cette question de la légitimité du contrôle et de l'abus de pouvoir. *«La question de la vie privée est politique : il n'y a pas de libertés sans vie privée. La protection de la vie privée passe également par la préservation du droit de s'opposer à une autre forme de société»(2).*

Pour les entreprises, le développement du web participatif, des applications pour smartphones, de la publicité comportementale et des outils intelligents connectés constituent un véritable eldorado informationnel sur les consommateurs. Les cartes de fidélité incitent les clients, en échange de magnifiques assiettes en céramique, à céder leurs données et à déclarer leurs achats. L'utilisation d'une application « lampe de poche » exige pour être installée l'accès à l'ensemble des contacts de l'utilisateur. Votre e-frigo passe automatiquement la commande des denrées manquantes. Sans parler des réseaux sociaux, livres volontairement ouverts sur votre personnalité et où vos goûts sont scrutés via vos «like» par les sociétés de marketing (et la NSA, par ailleurs...). Si l'Union européenne tente (timidement) d'améliorer la protection des données personnelles des citoyens (droit à l'oubli, privacy by design...), elle développe parallèlement des instruments de surveillance et d'échange des données à l'usage des services de renseignement et de police qui mettent en péril cette vie privée. Une ambiguïté qui appelle à la vigilance et impose une question : les citoyens doivent-ils accepter la violation de leur vie privée pour être mieux protégés ?

Les médias participent également à cette fragilisation de l'intime. Une certaine presse, peu scrupuleuse d'éthique, rend particulièrement poreuse la frontière entre la vie privée et la vie publique des hommes politiques et autres personnages médiatiques avec le risque de décrédibiliser la fonction, de permettre aux discours populistes de donner de la voix et à la démocratie de perdre la sienne. Sans parler de la télé-réalité mettant en scène de manière peu reluisante les vies de citoyens lambda en prime-time. Avec, à l'horizon, un estompement de la norme en matière de dignité humaine et une normalisation du voyeurisme et de l'exhibitionnisme comme instrument de divertissement.

Enfin, stimulés par les extraordinaires performances d'une technologie omniprésente dans les objets du quotidien, et en particulier les smartphones, les utilisateurs oublient parfois que cette technologie, souvent présentée comme gratuite, a un coût caché. Celui de leurs données personnelles d'une valeur inestimable pour les sociétés de marketing.

La vie privée, ce «droit d'être laissé seul», n'est pas un droit absolu. Elle peut être limitée pour des raisons légitimes, par exemple de sécurité ou encore, à titre plus individuel. Nonobstant ces exceptions, elle constitue une valeur fondamentale cardinale d'autant plus importante que l'effectivité d'autres droits, comme les libertés d'expression, d'opinion, de circulation ou de manifestation sont dépendantes du respect de ce droit à la vie privée. Comme le disait Benjamin Franklin «*Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux*».

(1) Article 8 de la Convention européenne des droits de l'homme.
(2) «Souriez, vous êtes fichés. Big Brother en Europe» de Raf Jespers, Couleurs Livres, 2013.

LA VIE PRIVÉE SUR LE SITE DE LA LDH

Quelques documents intéressants

- http://www.liguedh.be/les-fichiers-audio-video-de-la-ligue-des-droits-de-lhomme/2105-1984-retour-vers-le-present-le-debat

- protection de la vie privée à l'égard des traitements de données à caractère personnel http://www.liguedh.be/images/PDF/documentation/positions_de_la_ligue/091013_avis_ldh_proposition_de_loi_modifiant_loi_08_12_1992.pdf

- Critique du projet de loi relatif à la gestion de l'information Policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle http://www.liguedh.be/images/PDF/documentation/analyses_juridiques/2013_analysecritique_bng_ldh.pdf

- PRISM : un échelon plus loin http://www.liguedh.be/les-documents-des-commissions-thematiques/1770-prism-un-echelon-plus-loin

- Directive Data Retention : position et enjeux http://www.liguedh.be/toutes-les-activites-de-la-ligue/1757-transposition-de-la-directive-europeenne-sur-la-conservation-des-donnees-un-danger-pour-la-vie-privee-et-la-democratie

D'autres documents sont disponibles sur le site www.liguedh.be/72430 rubrique Documents

Helena ALMEIDA, chargée de communication LDH

Violences conjugales : les limites du respect de la vie privée

Le respect de la vie privée doit s'effacer lorsque l'intimité donne lieu à des violences conjugales ou familiales. Ce droit fondamental ne peut être détourné par les agresseurs pour être un paravent à leurs actes.

La violence conjugale a été officiellement définie à l'occasion de la Conférence interministérielle belge de 2006 : «*Les violences dans les relations intimes sont un ensemble de comportements, d'actes, d'attitudes de l'un des partenaires ou ex-partenaires qui visent à contrôler et dominer l'autre. Elles comprennent les agressions, les menaces ou les contraintes verbales, physiques, sexuelles, économiques, répétées ou amenées à se répéter portant atteinte à l'intégrité de l'autre et même à son intégration socioprofessionnelle.(...)*»

L'intimidation et le harcèlement psychologique, les agressions verbales et physiques (y compris l'obligation sexuelle - non, ce n'est pas un «devoir» conjugal) peuvent concerner n'importe qui, à tout âge, dans tout type de structure. Ni la religion, ni le statut social ou économique n'entrent en ligne de compte, pas plus que le sexe, contrairement aux idées reçues, bien que les femmes soient, dans une écrasante majorité, les victimes.

Des conséquences dramatiques À l'échelle mondiale, la violence conjugale est la forme la plus courante de mauvais traitements exercés envers les femmes. Une étude multipays de l'OMS(1) a pointé des chiffres effrayants, notamment sur le nombre de cas qui surviennent durant la grossesse. Une autre enquête(2) a dévoilé récemment qu'une femme sur trois en Europe a subi des sévices physiques ou sexuels (depuis l'âge de 15 ans). En Belgique, ce chiffre se vérifie également (36%) et les violences d'ordre psychologique montent même à 43% au sein de l'Union Européenne.

Les conséquences de ces comportements peuvent s'avérer extrêmement graves, voire mortelles : dépressions, suicides, assassinats. Difficile de mesurer les séquelles émotionnelles pour les personnes touchées et leur entourage, avec les enfants en première ligne. Parallèlement aux dégâts individuels, les coûts sociaux se révèlent importants en termes de soins de santé, d'actions des services sociaux, de justice pénale et, plus cyniquement, de productivité sur le lieu de travail.

Devoir d'intrusion Face à ces situations dramatiques, le devoir de protection des personnes l'emporte, dans ce cas bien précis, sur le droit à la vie privée. L'interférence dans la sphère intime est d'autant plus justifiée que la plupart des femmes (et des hommes) gardent le silence sur ce qu'elles subissent. Longtemps sourds et muets, les citoyens et la société, indifférents, complices ou impuissants, sortent depuis quelques années de leur réserve et discrétion à l'égard du cercle familial, sous l'impulsion de mouvements féministes et d'associations de défense des victimes.

À présent, ces délits sont punissables par la loi et les pouvoirs publics belges ont investi cette matière, notamment en ratifiant en 2012 la Convention d'Istanbul, d'application depuis le 1er août 2014, qui fixe des normes pour prévenir et combattre la violence envers les femmes. Depuis 2001, des Plans d'action ont aussi été mis en place par le gouvernement fédéral, suivi par la région Wallonne en 2005. Un an plus tard, la circulaire «Tolérance zéro» a été étendue à l'ensemble des Parquets du pays pour lutter contre les brutalités au sein du couple.

Les campagnes de sensibilisation menées par les associations sont tout autant primordiales pour informer les victimes et les témoins. La formation des intervenants est également indispensable pour accueillir les déclarations et accompagner les personnes (secteur associatif, social, services de police...). Mais aussi et surtout une meilleure promotion générale des relations égalitaires et un combat contre les attitudes patriarcales et machistes : l'agressivité constitue un moyen de contrôle prenant ses racines dans le rapport de pouvoir stéréotypé et inégal entre l'homme et la femme.

Dans ce cadre-là, le droit à la vie privée offre un écran de protection aux bourreaux qui peuvent agir en toute impunité, et un rempart d'invisibilité et de silence qui maintient les victimes en enfer. Les violences familiales doivent donc être mises en lumière sur la scène publique pour pouvoir être dénoncées et punies.

(1) Téléchargeable sur www.who.int/gender/violence/who_multicountry_study/summary_report/summaryreportfrenchlow.pdf
(2) http://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance_fr_0.pdf



Laurie Phillips, Présidente ad interim de la Commission Nouvelles Technologies LDH

Législation européenne et belge sur la vie privée

En matière de vie privée, il y a indubitablement un avant et un après 11 septembre 2001. Comment trouver un juste équilibre entre lutte contre le terrorisme et respect des libertés fondamentales ?

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.
Article 7 de la Charte des droits fondamentaux de l'Union européenne

Toute personne a droit à la protection des données à caractère personnel la concernant.
Article 10 de la Convention européenne des droits de l'Homme

Après la seconde guerre mondiale, un large mouvement européen en faveur de la reconnaissance de libertés considérées comme universelles et fondamentales s'est développé. C'est ainsi que la Déclaration universelle des droits de l'Homme (1948), puis la Convention européenne des droits de l'Homme (1950) et le Pacte relatif aux droits civils et politiques (1966) virent le jour: ces textes européens et internationaux mirent l'accent sur le respect des libertés fondamentales, considérées comme liées à l'essence même de l'être humain. Parmi celles-ci, figuraient le respect de la vie privée et une liberté fondamentale dont l'effectivité lui est intimement liée : la liberté d'expression. Depuis les années 50, donc, chaque citoyen européen a pu légitimement croire que sa vie privée était protégée et que toute ingérence serait punie si elle ne respectait pas les conditions très strictes liées aux rares exceptions légalement justifiées.

Est-ce à dire qu'il n'y a pas eu d'actes terroristes entre les années 1950 et les années 2000 ? Non bien sûr. Mais la réponse qui était apportée à cette problématique n'était pas du tout la même que celle qui lui est donnée aujourd'hui. La Convention européenne pour la Lutte contre le terrorisme (1977) définissait le terrorisme de manière stricte en énonçant précisément les actes («utilisation de bombes, de grenades (...)») entrant en considération dans cette définition. Les années 90 virent la promulgation de la Directive 95/46 dite «vie privée». Grâce à cette directive, tout traitement de données à caractère personnel devait répondre à des conditions bien précises qui protégeaient le citoyen des intrusions dans sa vie privée...

Mais tout bascula avec les attentats du 11 septembre 2001.

Tous (potentiellement) coupables ? Comment rassurer la population ? Il fallait, du point de vue des autorités, répondre vite et fort. Alors, il se mit à pleuvoir quantité de textes dont l'objectif n'était plus de défendre nos libertés fondamentales mais bien de «lutter contre le terrorisme», quitte à affaiblir voire étouffer certaines de ces libertés fondamentales. La Décision cadre du Conseil européen du 13 juin 2002 (2002/475) donna une nouvelle définition au terme «terrorisme». Une définition très large qui envisage tous les citoyens comme autant de suspects potentiels. Une définition tellement large que les marges d'interprétations rendent désormais envisageable l'intégration des syndicats et d'acteurs du monde associatif dans cette définition dès lors que leurs revendications et actions (la production d'un prospectus ou d'un pamphlet remettant en cause les structures sociales) pourraient «déstabiliser une structure politique».

Dans le même mouvement sécuritaire, l'adoption de la Directive 2002/58 rendait possible la rétention des données, ce que de nombreux Etats membres, dont la Belgique, s'empressèrent de faire. Mais cette possibilité devint, quatre ans plus tard, une imposition. Car, entretemps, les attentats de Madrid (2004) et de Londres (2005) durcirent encore le mouvement sécuritaire, entre autres, en organisant la coopération transfrontalière (Traité de Prüm) «notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale». Désormais, furent notamment autorisées la consultation et la comparaison automatisées de données à caractère personnel en ce compris l'ADN...

Et une nouvelle Directive consacrée à la rétention de Données (2006/24) imposa à tous les Etats membres, via leurs opérateurs de télécommunication, de conserver, pendant une période de six mois à deux ans, les métadonnées des échanges. Il est vrai que rien n'est conservé sur le contenu des échanges. Mais les informations recueillies (lieu et durée d'appel/de l'échange, personnes contactées...) permettent d'obtenir une image précise et complète de la vie aussi bien privée que professionnelle de tous les citoyens européens.

C'était fait : tous les citoyens étaient désormais considérés comme «suspects» potentiels. Cette directive fut transposée à tort et à travers à travers les différents Etats membres. Si bien que le rapport de la Commission européenne établit, en 2011, que la plupart des États membres autorisaient l'accès aux données conservées et leur utilisation pour des finalités dépassant celles couvertes par la directive et que le droit à la vie privée n'était pas respecté. En 2013, le Contrôleur européen de la protection des données (CEPD) rendit lui aussi un rapport selon lequel la nécessité de la rétention des données prévue par la Directive 2006/24

n'était pas démontrée à suffisance et, qu'en outre, elle manquait de «prévisibilité» et attentait au respect de la vie privée.

La Cour de justice européenne fut saisie et tant l'avocat général (Villalon Cruz 2013) que l'arrêt qui fut rendu le 08 avril 2014 (C 293/12) conclurent que la Directive 2006/24 comportait deux ingérences au respect de la vie privée : la rétention des données elle-même et l'accès que les autorités nationales s'étaient arrogé.

Un mouvement de libertés ? Le principe de proportionnalité qui prévaut depuis les années 50 et qui persiste encore aujourd'hui exige que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs. La directive 2006/24 ne respecte pas ce principe.

Cet arrêt est-il le signe qu'un nouveau mouvement s'annonce ? Aura-t-il une influence sur le futur Règlement européen sur la protection de la vie privée? A l'heure où les attentats de Paris relancent le renforcement du processus sécuritaire, la LDH rappelle que si la lutte contre le terrorisme est indispensable, elle doit impérativement maintenir le délicat équilibre entre le respect des libertés fondamentales, parmi lesquelles le respect de la vie privée, et l'intérêt légitime de sécurité.

Droit à l'oubli numérique

La directive 95/46 dite « vie privée » établit les droits dont disposent les citoyens lorsque leurs données à caractère personnel sont traitées. La loi du 08.12.1998 qui transposa cette directive en droit belge reconnaissait notamment que les données ne pouvaient pas être conservées ad vitam aeternam.

Le 13 mai 2014, la Cour de justice européenne a rendu un arrêt reconnaissant les moteurs de recherche (Google, Yahoo…) comme « responsables de traitement » et leur a imposé l'obligation de ne conserver les données à caractère personnel que durant le temps nécessaire et proportionné, consacrant ainsi le droit à l'oubli numérique. Grâce à cet arrêt, les citoyens européens ont désormais la possibilité de demander, moyennant certaines conditions (entre autres, apporter la preuve que le maintien de l'accès à ces informations leur est dommageable, que leurs données à caractère personnel n'apparaissent plus dans les résultats de moteurs de recherche en ligne. Il est vrai que certaines informations présentes sur la toile pouvaient constituer un frein, par exemple, à la réinsertion d'un détenu ayant purgé sa peine, à une personne citée dans la presse dans le cadre d'une affaire judiciaire et ayant obtenu un non-lieu ou, comme ce fut le cas en Allemagne, une victime d'abus sexuel souhaitant que son nom disparaisse des articles traitant de son affaire.

Suite à sa condamnation, Google, le plus célèbre des moteurs de recherche, a mis en ligne un formulaire. Les demandes concernant l'oubli numérique se sont multipliées depuis lors à travers toute l'Europe. Rien qu'en Belgique, plusieurs milliers de personnes (5000 en octobre dernier) ont déjà introduit une demande auprès de l'opérateur. Toutes les demandes ne sont évidemment pas recevables. C'est le cas lorsque des « hommes publics », des responsables de banques ou des hommes politiques tentent d'utiliser ce droit afin d'effacer les traces des scandales auxquels ils ont été mêlés (déboires financiers, condamnations judiciaires…).

Ce droit à l'oubli numérique peut poser légitimement question dans le chef, par exemple, des historiens et des archivistes qui risquent de perdre une source non négligeable d'informations, il constitue néanmoins une avancée considérable quant à la possibilité pour les citoyens de reprendre la maîtrise de leurs données personnelles.

Manuel Lambert, conseiller juridique LDH

Violence des échanges de données en milieu tempéré

Trop de données tuent-elles les données… avec, en victime collatérale, la vie privée des citoyens ?

Petite expérience de physique des droits humains : la conjonction des deux facteurs distincts suivants va avoir un effet centrifuge sur les droits fondamentaux. D'un côté, certains individus qui semblent avoir une conscience limitée des conséquences possibles de la publication de photos personnelles ou de certains commentaires sur le web. De l'autre, des pouvoirs publics et privés avec un appétit vorace pour ce genre de données. (On peut d'ailleurs s'interroger sur l'intérêt de collecter une quantité aussi démesurée de données pour exercer leurs missions. A titre d'exemple, pour constituer un passeport biométrique, le citoyen belge doit donner pas moins de 20 données à caractère personnel : numéro de GSM, adresse électronique… En quoi ces données sont-elles nécessaires pour établir un passeport?). Le résultat de cette conjonction est explosif.

Données à go-go Pour lutter contre la criminalité en général et le terrorisme en particulier, les autorités procèdent depuis une vingtaine d'années à des collectes aussi massives que systématiques de données à caractère personnel dont l'objectif déclaré est d'améliorer cette lutte. Les législations se sont multipliées pour permettre aux divers services répressifs de mener à bien leurs missions. Si l'on peut comprendre la nécessité pour ceux-ci de disposer de données adéquates et pertinentes, on peut douter que ces collectes généralisées permettent d'atteindre cet objectif.

Outre la question de leur efficacité (une analyse sérieuse de milliards de métadonnées issues de communications électroniques et téléphoniques n'est-elle pas illusoire ?), la légitimité et la légalité de ces collectes sont extrêmement questionnables. Et questionnées.

La directive européenne relative à la rétention des données (lire article page 7) constitue une illustration d'une dérive de ce type de collecte massive, où l'on passe du principe de la surveillance des seules personnes suspectes d'infraction à la surveillance généralisée de toutes et tous, sans distinction.

En Belgique, l'année 2014 a vu la consolidation du fichage policier, via l'adoption de la loi du 18 mars 2014 relative à la gestion de l'information policière, qui a légalisé l'existence de la BNG, c'est-à-dire la Banque de données Nationale Générale. Si cette législation a le mérite de donner une base légale à des fichiers policiers qui préexistaient et étaient largement utilisés (le journal Le Soir a fait état du fichage de 1,6 millions de personnes dans cette base de données, soit plus d'un dixième de la population…), elle pose de sérieuses questions quant à la protection des droits fondamentaux des individus qui s'y trouvent inscrits (contrôle a priori sur l'inscription de ces données en BNG, droit de recours du citoyen, etc.). C'est la raison pour laquelle la LDH a décidé de demander à la Cour constitutionnelle d'annuler certains articles de cette loi qui sont clairement en contradiction avec les droits fondamentaux des individus qui se retrouvent fichés, dans certains cas alors même qu'aucune infraction ne leur est reprochée.

Mesures mesurées ? Enfin, à l'heure où nous écrivons ces lignes, on peut pronostiquer, même sans en connaître encore précisément la teneur, que les mesures de renforcement de la lutte anti-terroriste qui ont suivi les attentats de Paris risquent d'avoir une incidence sur le respect de la vie privée. On peut notamment déjà pointer la proposition de créer un fichier européen de données de passagers des compagnies aériennes (ou « Passenger Name Record », PNR) qui, bien que déposée dès 2011 par la Commission européenne et entérinée par les Etats membres en 2012, va connaître un coup d'accélérateur.

L'extension de la liste des infractions donnant lieu à l'utilisation des méthodes particulières de recherche et l'échange d'informations font également partie de ces mesures. Si elles peuvent sembler logiques dans le contexte actuel, elles ne sont en réalité pas indispensables, l'arsenal législatif existant ayant déjà été très amplement élargi ces dernières années. Par ailleurs, les personnes concernées par ce type de surveillance sont déjà connues par les services compétents. Quoiqu'il en soit, ces mesures doivent rester proportionnées, afin d'éviter des effets potentiellement pervers – et prévisibles -, effets qui se répercuteraient sur l'ensemble des citoyens et pas seulement sur les terroristes ou présumés tels.

Dans ce contexte, l'accessibilité de nombreuses données personnelles et la revendication d'un droit à la sécurité, largement exploitée par les acteurs publics et privés, aboutissent à une limitation de plus en plus conséquente du droit au respect de la vie privée des citoyens. Est-ce qu'il en résulte une plus grande sécurité de ces derniers pour autant ? Cela reste à démontrer…

John Pitseys, chargé de recherche au CRISP

Vie privée et sécurité : qu'est-ce qu'une position libérale ?

La protection de la sécurité publique justifie-t-elle de limiter les droits individuels, parmi lesquels le droit à la vie privée ? Dans le débat public, le droit à la vie privée est parfois opposé à ce qu'on appelle aujourd'hui «le droit à la sécurité», qu'il s'agisse de souligner que ce dernier est après tout le premier des droits individuels ou, au contraire, de critiquer les dérives sécuritaires. Encore faut-il que cette opposition soit pertinente.

Pour le libéralisme politique, la liberté individuelle est une forme de propriété de soi. A l'inverse, la propriété est, comme l'écrirait Locke, une prolongation de la liberté individuelle : c'est dans ce cadre que la sûreté des personnes fut affirmée comme un droit «naturel et imprescriptible» dès la Déclaration des droits de l'homme et du citoyen de 1789. Le droit à la sûreté répond à une exigence fondamentale, car il vise à protéger les citoyens contre les arrestations et les emprisonnements arbitraires de la part des autorités. Toute personne a droit à la liberté, et toute personne arrêtée a le droit de connaitre les raisons de son arrestation. Déjà inscrite en 1215 dans la Grande Charte, la notion d'Habeas corpus impose que toute personne arrêtée soit présentée dans un délai bref devant un juge, ce dernier vérifiant que l'arrestation a bien un fondement solide. Aujourd'hui encore, le droit à la sûreté est censé encadrer les contrôles d'identité, les fouilles au corps, les détentions provisoires.

Toutefois, l'idéal de liberté individuelle ne justifie pas seulement le droit à la sûreté, mais aussi une des formes les plus élémentaires de la propriété de soi : le droit de garder son quant à soi. Dans les théories du contrat social, l'homme est son propre propriétaire car il est considéré capable de former et de diriger sa volonté de manière autonome. Dans ce cadre, le droit à la vie privée et le droit à la sûreté sont conçus sur le même patron philosophique. Ces droits garantissent tous deux l'individu contre les immixtions abusives du pouvoir – et de l'Etat en particulier. Il n'y a pas de sûreté de l'individu sans protection de sa sphère personnelle et intime. Et pas de respect possible de la vie privée si l'Etat peut agir de manière arbitraire.

De la sûreté à la sécurité La signification du droit à la sûreté a toutefois évolué, avant d'être progressivement subvertie. D'une part, le droit à la sûreté s'est élargi pour désigner également la protection de l'intégrité personnelle des citoyens, contre l'Etat mais aussi contre les activités délictueuses commises par des particuliers. A ces fins, il est demandé à l'Etat de remplir des fonctions de police. Toutefois, celles-ci ne sont pas a priori contradictoires avec le respect de la vie privée. La sûreté des personnes comprend également celle de leur domicile, de leur correspondance, de leur vie familiale. L'enquête sur les crimes est censée être dissociée des fonctions de renseignement. Pour le reste, le droit au respect de la vie privée peut bien sûr connaitre des restrictions, mais ni plus ni moins que les autres droits fondamentaux.

D'autre part, le droit à la sûreté s'est progressivement mué en droit à la sécurité. Les deux termes semblent voisins puisqu'ils ils expriment chacun l'idée qu'il est légitime de protéger l'intégrité des personnes. Toutefois, ils recouvrent en réalité un champ d'application et une signification différente. La sûreté désigne un droit individuel, associé à la protection de la personne. Concept flou, la sécurité désigne un état de la société, associé à un idéal d'ordre public. Pour Ole Waever, la notion de sécurité distingue et agrège deux sens différents : la sécurité nationale et la sécurité sociétale. La première aurait trait à la souveraineté et à la survie du régime, et la seconde concernerait l'identité et la survie de la société. La sécurité sociétale est ainsi présentée comme «la capacité d'une société à persister dans ses caractéristiques essentielles face aux conditions changeantes et face à des menaces probables ou réelles». Elle désigne ce faisant les dispositifs visant à contenir les facteurs internes de déstabilisation de la société, qu'il s'agisse de l'insécurité, des incivilités, des risques sanitaires, des troubles créés par l'intégration des communautés migrantes, de la perte des valeurs culturelles et des styles de vie, etc. Dans ce cadre, la lutte contre le terrorisme recouvre à la fois la notion de sécurité nationale et de sécurité sociétale : elle doit assurer la pérennité de la communauté, et libérer la société des risques qui pèsent sur elle.

La manière dont la notion de sécurité construit performativement ses propres objets – menace réelle ou menace construite, faits d'insécurité et sentiment d'insécurité - a déjà été amplement débattue. Ce qui importe ici, c'est de comprendre que la notion de sécurité transforme profondément l'objet et la philosophie du droit à la sûreté. La sûreté est conçue comme un droit, qu'une politique de sécurité contribuera à garantir. La sécurité est soit un projet politique et policier de gestion des risques et de maintien de l'ordre public (sécurité sociétale), soit un prolongement de la logique de guerre au sein de la communauté politique (sécurité nationale). Dans ce cadre, affirmer que la sécurité est «le premier des droits fondamentaux » est un contre-sens compréhensible mais profond. La sécurité ne vise pas à protéger le citoyen mais à défendre la société: elle ne désigne pas un droit mais un objectif politique.

Le droit à la vie privée et le droit à la sûreté sont compris comme des droits individuels qu'il s'agit de marier si c'est possible, et d'articuler de manière discursive quand c'est nécessaire. La logique de sécurité n'accorde par contre aucune valeur particulière au respect de la vie privée. Elle n'accorde d'ailleurs qu'une valeur instrumentale aux droits fondamentaux et aux institutions démocratiques : le respect des droits et le bon fonctionnement des institutions sont des objectifs qui doivent être poursuivis s'ils permettent d'assurer la paix sociale.

Cela signifie-t-il que la sécurité est un principe à rejeter ? Non ; cela implique que l'équilibre à trouver entre sécurité et vie privée n'est pas un équilibre entre deux droits qui se valent, mais un rapport asymétrique entre un bien social fondamental, celui de conserver et développer sa sphère intime et personnelle, et un objectif politique dont les contours et l'application doivent être justifiés en fonction des circonstances.

Gérer un rapport asymétrique Plusieurs types d'arguments peuvent être invoqués pour défendre la vie privée du citoyen. On peut estimer qu'il s'agit d'un droit individuel, d'une condition nécessaire à l'égalité de tous, vis-à-vis de l'Etat, mais aussi des pouvoirs économiques ou religieux, ou encore une question de dignité humaine.

A l'inverse, le culte de la raison d'Etat transcende les clivages philosophiques et partisans. Un conservateur cohérent considérera peut-être que le maintien de la cohésion sociale et la mise en place d'une police efficace justifie de limiter certains droit fondamentaux, parmi lesquels le respect de la vie privée. Peut-être même appuiera-t-il sa position sur les «valeurs démocratiques » et sur «l'esprit de liberté » du pays concerné, alors assimilés à des valeurs culturelles propres à la communauté. A contrario, rien ne permet de penser que les partis dits progressistes sont intrinsèquement plus attachés au respect de la vie privée : il convient ainsi de constater que les partis socialistes belges ont voté l'ensemble des lois antiterroristes promulguées depuis dix ans.

Mais, en tout état de cause, si on estime qu'une société juste doit garantir aux individus certains droits ou biens sociaux fondamentaux et que le respect de la vie privée en fait partie, cela signifie que le principe de sécurité et le respect de la vie privée ne peuvent être mis sur le même pied. Dans une société libérale, le devoir n'est défini qu'à partir des droits qui lui préexistent. Restreindre le droit à la vie privée n'est pas une simple affaire de jugement bien pesé, ou d'équilibre à trouver entre différents droits. Dans le cadre des politiques de sécurité, les restrictions au respect de la vie privée doivent être strictement limitées. À l'heure où il est question de compléter l'arsenal législatif déjà existant en matière de lois antiterroristes, cerner ce que peut être une position libérale en matière de sécurité permettra de mieux comprendre les choix que poseront les différents partis.

(1) Ole Waever, «Societal security : the concept» in O. Waever, B. Buzan, M. Kelstrup, P. Lemaître (éd.), Identity Migration and the New Security Agenda in Europe, New York, St Martin's Press, 1993.
(2) Ayse Ceyhan «Analyser la sécurité : Dillon, Waever, Williams et les autres », Sécurité et immigration, n°31-32, 1998, p. 5.

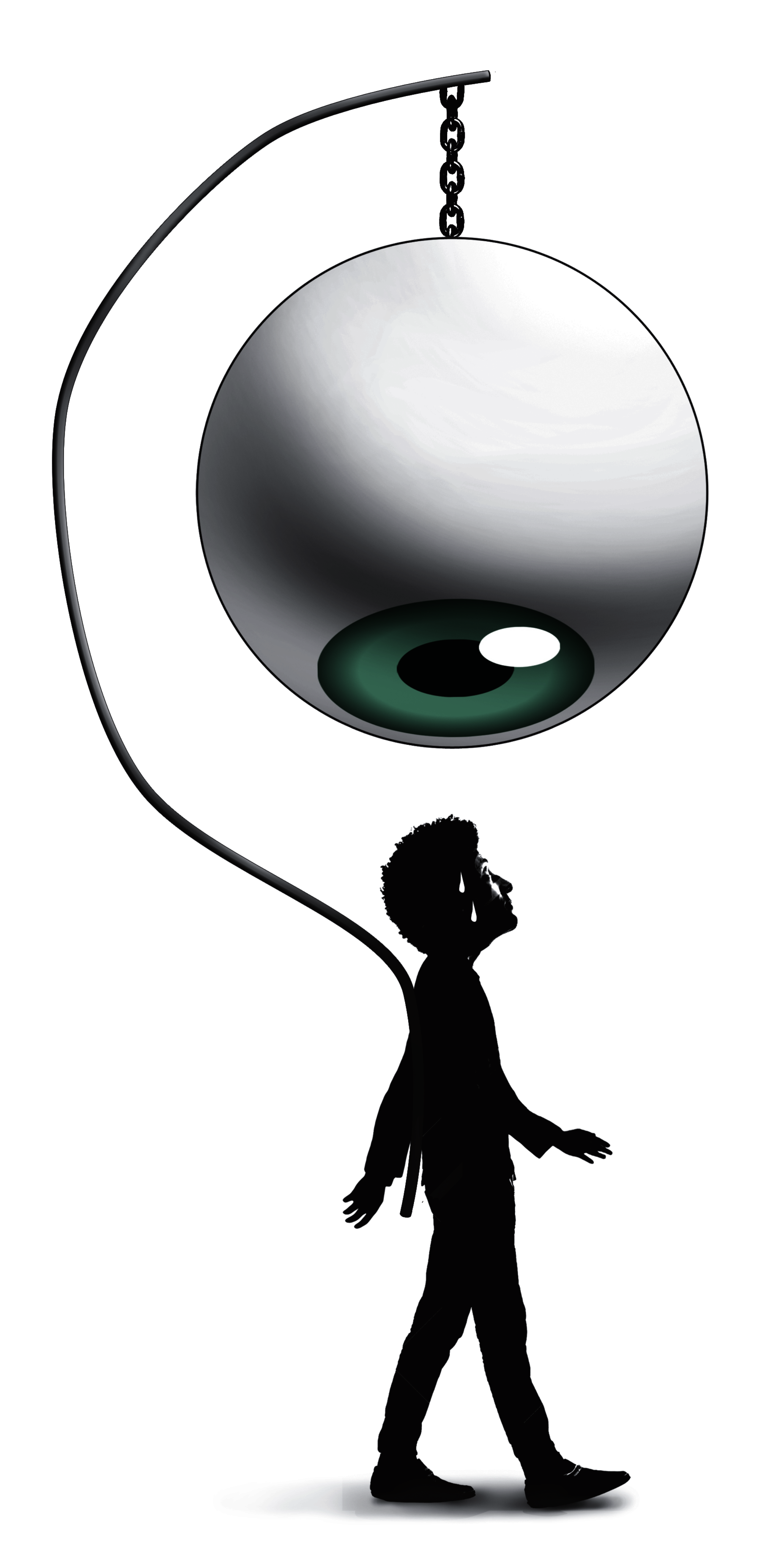


«La Zone du Dehors» de Alain Damasio, Folio SF, 2009, 651 pages

La zone du dehors

Que rêver de mieux qu'une société toujours à l'écoute de ses citoyens, prompte à répondre aux attentes de chacun, que celles-ci concernent leurs achats, loisirs, travail, confort ou sécurité. Les habitants de Cerclon I vivent dans un système de «social-démocratie» qui veille au bien-être de ses citoyens. Rien ne dépasse en 2084 (1984 ?) sur Cerclon I, planté sur un astéroïde en orbite autour de Saturne. Mais est-ce une société de rêve pour autant ? Ou plutôt, qui peut rêver d'une telle société et à qui peut-elle réellement profiter ? Car la surveillance y est constante et réussit le tour de force de faire croire à la population que cette surveillance, il la désire.

Alain Damasio, dans un style faisant virevolter la première personne narrative d'un antagoniste à un autre, emmène le lecteur face à lui-même et au prix de son confort. Combien de grignotages successifs de notre libre-arbitre et de notre vie privée faudra-t-il avant de se révolter ? Car tel est bien le thème central de ce roman qui, à l'analyse, est moins un roman de science-fiction qu'une anticipation d'une société déjà à notre porte.



Catherine Forget, Avocate, Chercheuse au CRIDS

L'art du détournement des objets à des fins de surveillance

Géolocalisation, vidéosurveillance, authentification, biométrie… les outils de surveillance s'invitent de plus en plus régulièrement dans les gadgets de notre quotidien. Sans en être forcément conscients, nous sommes l'objet voire les objets d'une surveillance globale constante.

La révolution informatique a eu pour incidence d'apporter un champ nouveau à la surveillance. Que cette dernière soit commerciale ou sécuritaire, les technologies permettent d'initier et de récolter une quantité incroyable de données grâce à des méthodes particulières. La géolocalisation d'une personne, c'est-à-dire la localisation d'une personne avec précision et en temps réel, peut s'effectuer au moyen d'un téléphone portable. En cherchant le réseau, l'appareil se connecte à des antennes relais déterminables, permettant de situer avec précision la personne et d'analyser ses déplacements. De même, le wi-fi permet de géolocaliser une personne. Un Smartphone se connecte à différentes bornes wi-fi, permettant de suivre les déplacements de l'individu. Les Global Positioning System (GPS) permettent eux aussi la géolocalisation des automobilistes, toutefois moins précisément car elle s'effectue par satellites. Soulignons cependant que ce «problème» sera résolu à bref délai. En effet, dès octobre 2015, les voitures vendues dans l'Union européenne seront équipées de «l'eCall», une petite boîte noire permettant d'alerter manuellement ou automatiquement les services d'urgence en cas d'accident localisant ainsi directement la voiture. L'objet a suscité certaines craintes, néanmoins l'Union européenne tente de rassurer, le système devrait rester «dormant» et ne s'activera qu'en cas d'incident évitant ainsi le «traçage» des automobilistes.

Transports peu privés L'eCall n'est pas le seul dispositif susceptible de surveiller les automobilistes, nos routes pullulent de caméras Automatic Number Plate Recognition (ANPR). Ces caméras détectent d'éventuelles infractions et reconnaissent automatiquement les plaques d'immatriculation. Elles peuvent également, sur base d'une liste noire, alerter les services de police si telle voiture n'est pas en ordre de contrôle technique. En outre, les piétons ne sont pas en reste. Dans un avenir proche, si ce n'est pas déjà le cas, d'autres caméras terniront encore nos rues. Par exemple, des caméras thermiques sont au point, détectant les changements de chaleur, et dès lors les corps humains. D'autres caméras intelligentes détectent les mouvements physiques ou les bruits suspects. Les utilisateurs de la Société de Transports Intercommunaux Bruxellois (STIB) munis d'une 'carte Mobib' ne sont également pas à l'abri d'un éventuel traçage. Cette carte de la STIB est en effet équipée d'une puce Radio Frequency Identification (RFID), permettant l'identification d'une personne à distance et l'enregistrement de ses données de déplacement. Les passeports biométriques comprennent également des puces RFID contenant des empreintes digitales et une photo. La biométrie s'appuie en effet sur des données biologiques ou physiologiques d'une personne pour permettre son identification.

Profilages Indépendamment de nos déplacements, notre vie intime, nos opinions politiques et culturelles sont dorénavant encodées au départ de notre ordinateur personnel. Outre une quantité incroyable de données révélées volontairement par les utilisateurs des réseaux sociaux, les opérateurs de télécommunication ont l'obligation d'enregistrer l'ensemble des métadonnées, c'est-à-dire toutes nos données générées par nos communications électroniques (liste de contacts, date, heure des échanges…), à l'exception du contenu des messages envoyés. En accédant à ces différentes données, les services répressifs peuvent établir des profils très précis des utilisateurs, leurs déplacements, leurs centres d'intérêts, etc… Les utilisateurs des smartphones étant en permanence connectés, les applications en ligne, agendas, plans des villes, réseaux sociaux sont autant d'informations collectées par les opérateurs télécoms et accessibles (sur demande) pour les autorités judiciaires.

Les nouvelles technologies sont nombreuses et la liste est encore longue… Admettant que le domaine sécuritaire «ne connaît pas la crise» et fait fi des études relatives aux risques pour la santé des mesures précitées – l'impact des ondes électromagnétiques sur notre santé…- le développement des gadgets sécuritaires n'en est qu'à ses débuts. Même si l'article 8 de la Convention européenne des droits de l'homme garantit le droit à la vie privée, et l'article 8 § 1 de la Charte des droits fondamentaux de l'Union européenne la protection des données à caractère personnel, ces droits ne sont pas absolus et le combat est ardu dans un domaine où les fantasmes sécuritaires et commerciaux ont le vent en poupe.

Gregoire Wallenborn, Chercheur à l'Institut de Gestion de l'Environnement et d'Aménagement du Territoire

Une hyperconnexion qui laisse des traces

Commençons par une expérience intéressante : installez Ghostery dans les modules ou extensions de votre navigateur web. Vous allez découvrir les mouchards qui captent les traces que vous laissez sur internet et pouvoir choisir de refuser de partager ces informations. Ce que montre cette petite expérience est le nombre étonnant d'entreprises sur le web intéressées par votre activité… et vos données.

Des données captées également via les téléphones mobiles, boîtiers TV, cartes bancaires, GPS, thermostats ou frigos intelligents, etc. Et ce n'est qu'un début puisqu'on nous annonce des compteurs «intelligents» pour l'électricité, le gaz et l'eau, l'internet des objets, un suivi médical on-line et des «smart cities» pleines de capteurs.

Les interconnexions entre les humains et les machines se multiplient à une vitesse vertigineuse. Chaque connexion laisse une trace qui alimente d'énormes quantités de données, le «big data». Sur base du traitement de cette information, les entreprises et les gouvernements modèlent les comportements des individus, souvent à leur insu. Les traces sont généralement enregistrées sans l'approbation claire des usagers, qui ne savent pas ce qui en est fait même si cela contribue à individualiser les services, à moduler leurs prix selon des paramètres obscurs et, plus généralement, à surveiller et singulariser une multitude d'individus.

Les débats juridiques autour du big data et de la société de surveillance qui se met progressivement en place concernent généralement la protection des données et le respect de la vie privée. Il est évidemment crucial de déterminer qui a le droit de détenir les données et qui doit surveiller qui dans une démocratie. Et il faut refuser avec force toute tentative d'agrégation globale des données qui permettrait d'établir le profil complet d'un individu. De même, la singularisation des individus et la modulation des prix des services interrogent les notions d'assurance mutualiste et de service public. Ce ne sont pourtant pas ces questions qui sont les plus importantes, car elles supposent que le fonctionnement actuel du droit n'est pas fondamentalement menacé. Or, c'est le sujet de droit qui est progressivement éliminé des pratiques numériques.

Algorithme de vie La gouvernementalité algorithmique – selon les termes d'Antoinette Rouvroy et Thomas Berns – s'impose comme un nouveau régime qui pose la question de ce qu'il faut entendre par une vie et un sujet de droit. Pour le comprendre, il faut se doter d'une définition générique de la vie en tant que processus. Que l'on regarde du côté de la théorie de l'évolution ou des processus d'apprentissage, la vie se perpétue par l'articulation de deux moments : variation et adaptation. Variation génétique et adaptation à un environnement donné ; essais et ratés ou succès. Mais la gouvernementalité algorithmique redéfinit l'adaptation et réduit la variation au prévisible en niant la créativité inhérente du vivant.

La multiplication des capteurs rend l'environnement actif de telle sorte que c'est celui-ci qui s'adapte en permanence à chaque individu, anticipant ses comportements et même ses désirs. A partir des corrélations de traces, analysées par des algorithmes, il devient possible de prédire avec une certaine probabilité les actions des individus. Les personnes ne sont plus jugées sur leurs actes mais sur leurs dispositions. Si ce jugement n'est pas juridiquement contestable - il demeure dans l'ordre du possible -, il définit néanmoins activement la situation pratique de la personne. Les décisions se prennent sur base de ce qui se fait plutôt que sur ce que la multitude d'usagers désireraient démocratiquement faire de leur environnement.

La gouvernementalité algorithmique se passe de la délibération, de la capacité à réfléchir et à discuter des situations qui nous intéressent, notamment à propos de notre environnement. Elle ne capture pas les variations intrinsèques aux corps et les significations que les corps peuvent leur donner, qu'elles fussent des échecs ou des réussites, des conflits ou des surprises. Du coup, elle fait apparaître des droits qui n'étaient jusqu'ici qu'implicites dans l'acte juridique. Droit à se faire oublier. Droit à pouvoir délibérer, à apprendre, à saisir sa propre évolution, individuellement et collectivement. Droit à donner une signification à ce qui nous arrive et à offrir la possibilité d'une prise sur son environnement.

Dans la mesure où les traces sont activement produites et façonnent une manière de faire société (avec les autres, les objets et l'environnement), la question démocratique est déplacée. Si nous voulons pouvoir préserver le droit d'imaginer collectivement la société dans laquelle nous voulons vivre, il est capital de déterminer quelles traces nous voulons laisser.

Raf Jespers, Avocat chez PROGRESS Lawyers Network et auteur de « Souriez, vous êtes fichés. Big Brother en Europe » (Couleur livres, 2013)

Les stratégies des acteurs privés et publics pour limiter la protection de la vie privée des citoyens

Il y eut d'abord « l'œil de Dieu » qui vous voyait partout, puis le « Watching You » inquisiteur de l'Oncle Sam. A présent, ce sont l'État et les entreprises privées qui vous tiennent à l'œil, par le biais des technologies « Big Brother » les plus modernes. Pour la première fois dans l'histoire, la révolution technologique et digitale de ces dernières décennies a rendu possible le contrôle total de la population. Les citoyens se rebiffent un peu, certains plus virulemment que d'autres, mais l'écrasante majorité d'entre eux est réduite au silence par des arguments – réels ou démagogiques – des « nouveaux Dieux ».

Le slogan « Celui qui n'a rien à craindre, n'a rien à cacher » fonctionne toujours, mais la rengaine commence tout de même à devenir un peu éculée. Les stratégies visant à s'approprier vos données personnelles deviennent plus sophistiquées, plus fines, plus globales.

Les banques en première ligne Prenons l'exemple de « La Banque qui vous voit ». Mi-2013 déjà, BNP Paribas et ING Pays-Bas ont suscité de l'émoi en annonçant leur volonté de partager les données de leurs clients avec des partenaires ou de les vendre à des publicitaires et des entreprises externes. Ils ont été rappelés à l'ordre... mais les banques ne se le tiennent pas pour dit. Actuellement, les banques belges investissent des millions dans les mégadonnées. À l'été 2013, la KBC en a même révélé le montant : 500 millions d'euros. Derrière les écrans, toutes les banques travaillent d'arrache-pied à l'élaboration de systèmes de données clients hautement technologiques. Elles épient les habitudes de leurs clients notamment lorsqu'ils surfent sur leurs sites et investissent leurs comptes Facebook et Twitter via des systèmes d'exploration des données de plus en plus puissants, avec pour but affiché un meilleur service aux clients : afin de pouvoir lui proposer une offre personnalisée aux moments-clés de la vie (un nouveau boulot, une nouvelle voiture ou maison...). Les collaborateurs de la banque disposent ainsi d'un tableau de bord reprenant les données personnelles des clients, afin d'optimaliser l'activité commerciale. Pour simplifier la vie de leurs clients, leur fournir des gadgets gratuits et utiles ? En réalité, pour élaborer leurs profils détaillés et cartographier leur ADN personnel afin de permettre un traitement des données visant la promotion d'un produit ou un marketing proactif. Avec un but sacré : pousser les chiffres de vente et les gains des banques – de manière pas toujours très subtile. En 2013, Belfius et la KBC ont lancé un livre de comptes digital afin que les clients puissent gérer leur budget de manière digitale. Utile pour les clients (naïfs) : fin 2013, rien que chez Belfius, 200.000 livres de comptes avaient été créés. Une opération très utile pour les responsables marketing de la banque.

Mines d'or La politique des banques illustre celle de toutes les entreprises privées, multinationales en tête. Les mégadonnées sont une mine d'or pour le commerce et la publicité : la possession, la recherche et l'utilisation des données personnelles sont devenus un élément essentiel de la lutte concurrentielle nationale et globale pour le marché. « Approcher des 'non-clients' sur la base de leur comportement sur le site Internet d'une banque est contraire à la loi », expose Willem De Beuckelaere, le président de la commission belge pour la vie privée[(1)]. Mais l'élaboration de profils clients à vocation commerciale, sur la base des données de clients propres « pour mieux vous servir », est également contraire à la loi sur la vie privée. Ce n'est pas parce que vous êtes client d'une banque ou d'un supermarché que ceux-ci ont le droit de traiter vos données dans n'importe quel but. Pour le traitement des données en vue d'une influence sur la consommation, la loi exige à juste titre le consentement explicite du client[(2)]. Le terme explicite implique que les petites lettres dans les contrats bancaires ne suffisent pas.

L'obligation des états de protéger les citoyens contre la terreur : quelles limites ? Les autorités agissent elles aussi de plus en plus directement dans la sphère de la vie privée. Les documents Snowden nous ont appris que la NSA et le GCHQ (les services secrets britanniques), en collaboration avec des entreprises, espionnent les données de presque toute la population de la planète. Aux États-Unis, la symbiose entre la NSA, les entreprises de technologies et la privatisation de la politique de sécurité est déjà bien avancée.

En Belgique aussi, les autorités mettent la vie privée sous pression, malgré l'institution par le gouvernement Michel Ier d'un secrétaire d'État à la vie privée, le libéral Bart Tommelein. La stratégie des États reposait, surtout depuis le 11 septembre, sur la lutte contre le terrorisme et la criminalité. La « stratégie de la terreur » faisait et fait encore appel à la préoccupation légitime des citoyens pour leur sécurité. Les États ont l'obligation de protéger leurs citoyens et d'éviter qu'ils soient victimes d'attentats terroristes. Nous constatons cependant que cette obligation est utilisée pour placer sous contrôle un public bien plus large que, par exemple, les seuls néo-nazis ou fascistes salafistes.

Ainsi, en 2006, après les attentats à Madrid et à Londres, la Commission européenne s'est attelée à une directive sur la rétention des données. Toutes les données de communications par Internet et téléphone des 500 millions de citoyens de l'UE devaient être conservées durant 6 à 24 mois pour les besoins de la lutte contre le terrorisme et les formes graves de criminalité. La Belgique a transposé la directive par la loi Turtelboom-Vande Lanotte du 30 juillet 2013, qui, sur différents points, va encore beaucoup plus loin que la directive. Par un arrêt historique du 8 avril 2014, la Cour de justice de l'Union européenne a annulé la directive[3], considérant qu'elle était disproportionnée et dépassait les limites de ce qui était strictement nécessaire dans la lutte contre la criminalité grave et le terrorisme. « Le citoyen a l'impression que sa vie privée est sous contrôle permanent », écrit la Cour. Cet arrêt n'a pas reçu l'attention qu'il méritait alors qu'il devrait devenir une bible pour toute action publique qui touche à la vie privée; cependant. Il a causé tout au plus une vaguelette dans la politique relative à la vie privée des pays membres de l'UE. Mais la loi belge n'a pas été retirée. Au contraire, le gouvernement Michel Ier a annoncé la création d'encore plus de banques étatiques de données… et leur couplage.

Contrôle radical La sécurité du citoyen demeure la base idéologique principale pour justifier l'intervention des autorités. L'attaque meurtrière du 7 janvier 2015 contre Charlie Hebdo à Paris va donner du poids à cette justification.

Ici aussi, cependant, la stratégie s'affine. Ainsi, la lutte contre la radicalisation devient un argument pour le contrôle étatique. Il est remarquable, à cet égard, que le premier ministre Charles Michel évoque « des radicalismes » au pluriel[4]. Celui qui pense que l'État vise uniquement - et à raison - les extrémistes islamistes ou nazis pourrait se fourvoyer : l'opposition sociale est également dans le collimateur. La lutte contre la fraude sociale est un autre argument récent pour demander l'accès à des données privées. La première action politique du secrétaire d'État Tommelein, compétent, outre la protection de la vie privée, pour la lutte contre la fraude sociale, fut sa résolution de contrôler la consommation en gaz, eau et électricité de quelques milliers d'allocataires sociaux isolés.

À bon droit, le citoyen attend des autorités publiques qu'elles lui garantissent une protection de sa vie privée. En 2014, des hackers ont volé les données de 152 millions de clients chez Adobe. La même année, aux États-Unis, c'étaient les données de 4,5 millions de patients des Community Health Services qui étaient volées[5]. Et ce ne sont que les sommets émergés de l'iceberg. Outre les autorités et les entreprises, l'accès aux mégadonnées est devenu un marché pour les criminels et les maîtres chanteurs. La protection contre la cybercriminalité ne peut cependant pas devenir un prétexte pour contrôler encore plus les citoyens.

Nous vivons à une époque où les acquis démocratiques, parmi lesquels la protection de la vie privée, sont mis sous pression. Ceux-ci ne peuvent être sacrifiés sur l'autel du commerce ou de la lutte contre le terrorisme. Toute stratégie en matière de vie privée doit partir de la primauté des droits fondamentaux. L'arrêt de la Cour de justice de l'Union européenne ne laisse pas subsister de doute sur cette prémisse nécessaire.

(1) De Standaard, 6-7 décembre 2014.
(2) Article 5 de la loi sur la protection de la vie privée.
(3) Arrêt de la CJUE, 8 avril 2014, C-293/12 et C-594/12.
(4) Mise à jour, RTBF, 5 janvier 2015.
(5) De Morgen, 3 janvier 2015, p. 24.

François Koeune et François-Xavier Standaert, UCL Crypto Group, Université catholique de Louvain

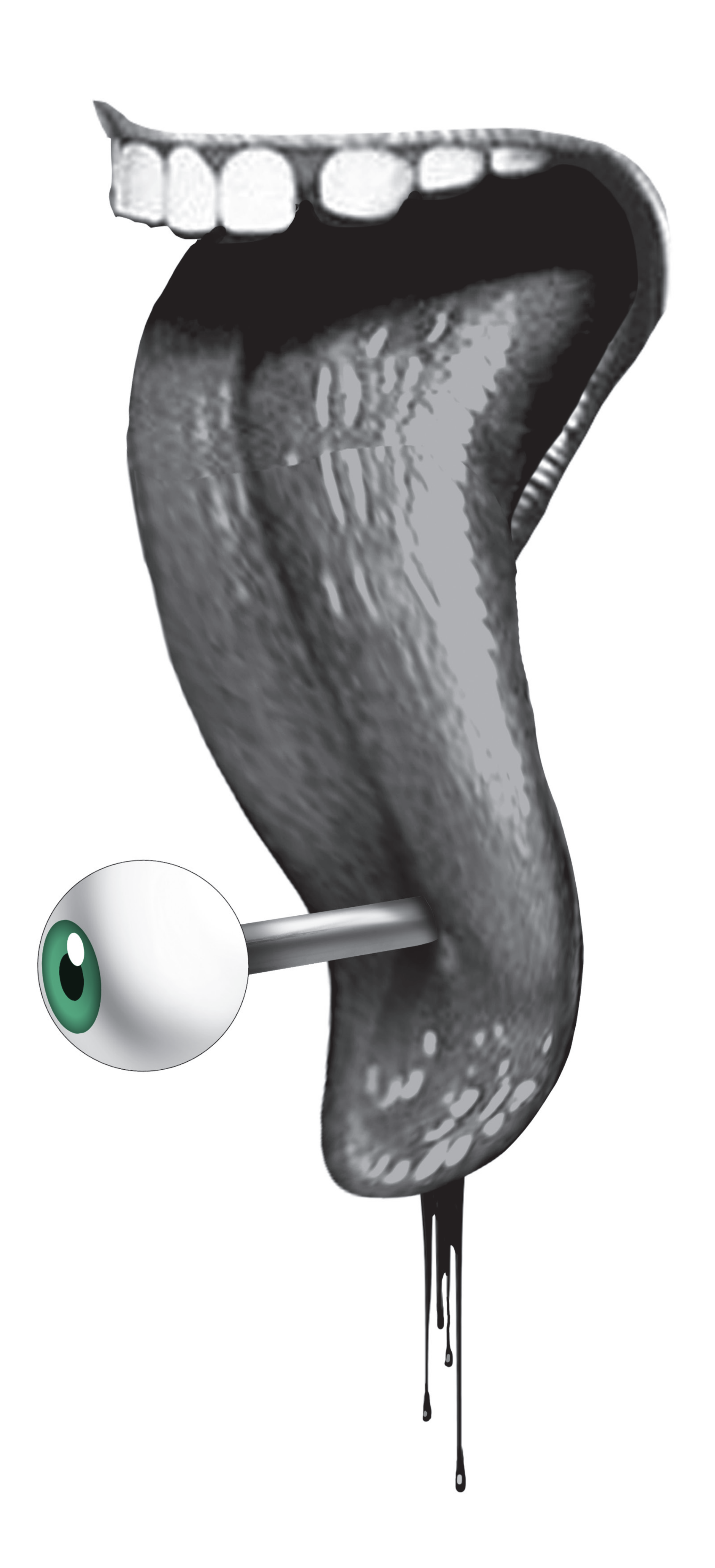
Sécurité des données et cryptographie : comment et pourquoi ?

Si l'utilisation de données précises sur des utilisateurs ou sur des modes de consommation peut s'avérer utile pour optimiser un certain nombre de services, elle pose également de nombreuses questions de sécurité. Démocratiser la cryptographie semble une des meilleures armes pour limiter les intrusions excessives dans notre vie privée. Illustrations…

Les outils cryptographiques les plus connus sont le chiffrement, qui protège le secret des données, et la signature, qui assure que les données sont authentiques. Prenons l'exemple du courrier électronique. Un premier pas indispensable pour améliorer ma vie privée consiste à chiffrer et signer les données durant leur transit entre le serveur mail et mon ordinateur. Ce faisant, je m'assure qu'aucun tiers malveillant ne peut lire ni modifier mon courrier tandis que je le rapatrie. Si cette première étape tend à se généraliser, il y a moyen d'aller plus loin. En traitant uniquement les données en transit, je me protège contre des tiers, mais je fais totalement confiance à mon fournisseur de mail, qui peut accéder à l'ensemble de mes données stockées sur ses serveurs. Des solutions commencent à apparaître qui proposent de sécuriser les emails dès leur création : l'auteur du mail le chiffre à mon intention et le fournisseur de mail se contente de stocker les messages chiffrés, sans pouvoir les lire ni les modifier. ProtonMail, récemment développé par des chercheurs de l'Organisation européenne pour la recherche nucléaire (CERN), est un exemple de cette tendance.

Authentification Une autre question liée à la vie privée est celle des informations à révéler lorsque je m'authentifie. Dans le cas de l'accès au mail, il est légitime que je prouve mon identité au serveur lorsque je désire accéder à mon courrier. Mais dans de nombreux cas, cela n'est pas forcément nécessaire. Supposons que je désire acheter une bouteille d'alcool. Le marchand pourra légitimement me demander de prouver que j'ai plus de 18 ans. Mais, en lui montrant ma carte d'identité, je lui révéle en fait beaucoup plus que ce qu'il doit savoir : mon nom, mon âge, ma nationalité… Dans l'absolu, on pourrait imaginer qu'un certificat attestant de ma majorité me soit délivré. Il comporterait une photo d'identité, mais aucune autre information me concernant. Une telle solution peut sembler extrême et trop coûteuse par rapport au bénéfice engendré. De nombreuses situations analogues existent cependant dans lesquelles la solution la plus respectueuse de la vie privée peut être mise en œuvre efficacement. La cryptographie offre des outils numériques, les protocoles à divulgation minimale, permettant de prouver que certaines conditions sont remplies, sans révéler aucune information supplémentaire. Grâce à ceux-ci, il est alors techniquement envisageable qu'une puce que je porte prouve que j'ai le droit d'utiliser un service sans pour autant révéler qui je suis à des tiers qui espionneraient les échanges ou au fournisseur de service.

Pourquoi se cacher ? Bien sûr, on peut se demander s'il est vraiment utile de vouloir ainsi cacher autant d'informations que possible dès lors que des possibilités techniques existent. En particulier, s'il est naturel de vouloir empêcher que des tiers puissent obtenir des informations, il peut paraître plus surprenant de vouloir limiter l'information au fournisseur de service légitime. Après tout, que m'importe que mon club de sport sache à quelle heure je suis arrivé? Nous voyons cependant deux raisons de procéder ainsi. D'abord, parce qu'il n'y a pas de raison de prêter plus de confiance que nécessaire au fournisseur (un peu de la même manière que je ne vais pas donner mon portefeuille au marchand en lui demandant de prendre la somme que je lui dois). Ensuite, et plus fondamentalement, parce que nous ne désirons pas forcément faire confiance en sa capacité de protéger les données qu'il reçoit. Protéger une base de données est une tâche complexe, et la presse rapporte régulièrement des cas de piratage où des entreprises voient les données qu'elles traitaient révélées sur internet. Même si lui-même n'en fait pas mauvais usage, mon interlocuteur peut mettre mes données en danger par son incapacité à les protéger correctement. En outre, des données élémentaires peuvent sembler totalement anodines, mais leur réelle portée doit être considérée dans l'optique du « big data » : l'agrégation massive de données anodines conduit à des informations très utiles, permettant un profilage très précis. De ce point de vue, la tendance actuelle, largement influencée par la multiplication des communications et la baisse du coût du stockage, semble être au « enregistrons tout, ne protégeons rien ». La cryptographie permet d'apporter des éléments en contrepoint : « révélons le minimum nécessaire, et protégeons-le de manière adéquate ».



Mathieu Beys, assistant à l'ULB et membre de l'Observatoire des violences policières de la LDH

Le droit à la vie privée : bouée de sauvetage des policiers violents et bâillon des témoins gênants ?

« Cette pauvre petite femme pleurait et criait, alors un groupe de personnes s'est levé pour protester contre les conditions de son expulsion (…). J'ai demandé aux policiers qu'ils soient un peu plus humains parce qu'ils menaçaient d'utiliser un coussin pour la faire taire mais ils m'ont remballée. Alors, j'ai sorti mon appareil pour faire des photos, en leur expliquant qu'elles serviront à un de mes collègues pour une future interpellation. Il m'a demandé d'arrêter et j'ai dit non (…) Nous avons été débarqués violemment par la police, sans que je n'aie eu le temps de prendre mes bagages ni mes chaussures. Lorsque je l'ai fait remarquer, l'un des agents m'a donné un coup au visage ».

Témoignage de Gisèle Mandaila, cité par Ch. V.,
« Putch contre une expulsion », 7 dimanche, 16 février 2014, p. 3.

Ce témoignage d'une députée bruxelloise illustre une tendance lourde identifiée par l'Observatoire des violences policières : de nombreux de policiers ne supportent pas d'être filmés pendant leur service, surtout lorsqu'ils risquent de déraper.

Fin août 2014, deux policiers brugeois ont porté plainte contre un citoyen qui avait filmé une banale intervention à la terrasse d'un café. L'incident a fait la une des médias relayant la thèse de certains syndicats policiers : les fonctionnaires ont aussi droit à une vie privée et il serait interdit voire punissable de les filmer sans leur accord. Ils pourraient même saisir le GSM du citoyen trop curieux. Les deux policiers soucieux de leur image ont reçu le soutien ferme de leur chef de corps et aussi celui, certes moins franc, de la commissaire générale de la police fédérale qui a déclaré dans une interview à Het Laatste News, « comprendre » leur initiative parce que « personne n'aime être constamment filmé ». Outre le fait que c'est tout à fait faux (et illégal), les citoyens apprécieront la remarque à sa juste valeur, étant quadrillés par des dispositifs de surveillance de plus en plus sophistiqués (reconnaissance automatique des plaques d'immatriculation, caméras « intelligentes »…).

Deux images, deux mesures Les pouvoirs publics semblent se ficher de la vie privée des citoyens comme de leur premier caleçon lorsque ces moyens de surveillance sont braqués sur la population et alimentent des bases de données gargantuesques et interconnectées. Pourtant, la force des images a largement fait ses preuves, tant pour prouver des infractions commises par certains policiers que pour alerter le public. Il suffit de se remémorer les morts filmées de Sémira Adamu, étouffée en 1998 par un gendarme avec un coussin dans l'avion qui devait la rapatrier au Nigéria et, plus récemment, de Jonathan Jacob, tué par une intervention plus que musclée de la brigade spéciale anversoise alors qu'il était seul et nu dans une cellule du commissariat de Mortsel. Depuis lors, la police belge et, plus étonnamment, l'Inspection générale qui est censé la contrôler, refusent de filmer systématiquement les expulsions d'étrangers, comme le demande notamment le Comité de l'ONU contre la torture. Et pourquoi donc? « Notamment parce que cela poserait des problèmes de respect de la vie privée pour d'autres personnes présentes »[1].

La vie privée des policiers, et des autres voyageurs qui auront été probablement filmés par de multiples caméras dans l'aéroport et les trams, bus, métros qui y mènent (visibles en temps réels et conservées par des agents de sécurité privée et par la police), serait subitement menacée par quelques prises de vue centrées sur l'étranger expulsé dans l'avion (à usage exclusif des organes de contrôle et de la justice). Pas besoin d'être docteur ès privacy pour comprendre que cette justification est totalement grotesque et semble surtout cacher une volonté de limiter au maximum l'efficacité des contrôles des opérations d'expulsion.

Même s'ils ont évidemment droit à une vie privée comme chacun d'entre nous, les membres des forces de l'ordre ne sont pas des citoyens comme les autres. Le service public qu'ils rendent limite inévitablement leurs droits : interdiction de se présenter aux élections, de manifester publiquement leurs opinions politiques… Selon la Déclaration des droits de l'Homme de 1789, la force publique « est instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée ». Les policiers sont donc habilités à utiliser la force uniquement parce qu'ils le font au nom de l'Etat et pas pour eux-mêmes. Certes, ils peuvent dans certaines situations demander au public de ne pas prendre d'images, par exemple pour protéger la vie privée des personnes arrêtées ou de victimes. Mais en principe, les forces de l'ordre « doivent considérer comme

normale l'attention que des citoyens ou des groupes de citoyens peuvent porter à leur mode d'action. Le fait d'être photographiés ou filmés durant leurs interventions ne peut constituer aucune gêne pour des policiers soucieux du respect des règles déontologiques»[2].

Filmer un policier n'est pas un délit Des policiers qui invoquent leur droit à l'image pour interdire aux citoyens de filmer leurs interventions dans l'espace public, c'est un peu comme si le ministre des Finances invoquait sa vie privée pour empêcher le public de voir les chiffres du budget pour contrôler ce que le gouvernement fait de l'argent des contribuables. Un non-sens dans une démocratie. Une dangereuse tentative d'intimidation pour censurer journalistes, citoyens, et même parlementaires, qui veulent mettre le doigt, ou l'objectif, là où ça fait mal... Il faut rappeler que le fait de filmer les forces de l'ordre n'est en rien une infraction et que celles-ci n'ont pas le droit de saisir un téléphone portable uniquement parce qu'il a filmé une opération policière, encore moins de s'introduire dans ce téléphone et d'effacer des données qui y seraient contenues. La seule restriction admissible concerne la diffusion de ces images : les policiers ne peuvent être identifiables. A défaut, on risquerait en effet de violer certains de leurs droits. Mais la prise d'image n'est en rien une infraction, ni la diffusion si les policiers ne sont pas identifiables. Au contraire, ce faisant, le citoyen participe au contrôle indispensable en démocratie qui doit s'exercer sur les pouvoirs publics. Par les temps qui courent, ce n'est pas inutile de le rappeler...

(1) Comité contre la torture de l'ONU, Examen du rapport soumis par la Belgique, CAT/C/BEL/3, 19 novembre 2012, § 52.
(2) Commission nationale de déontologie de la sécurité (CNDS) en France, Avis du 5 avril 2006, saisine n° 2005-29, Rapport annuel 2006, p. 32, http://cnds.defenseurdesdroits.fr/rapports/annuels.html.

Souriez, vous êtes fichés, Big Brother en Europe



«Souriez, vous êtes fichés, Big Brother en Europe» de Raf Jespers, Éditions Couleur livres, 2013, 224 pages

«Souriez, vous êtes fichés, Big Brother en Europe» explore les dix dernières années sous l'angle des menaces que portent en elles certaines utilisations qui sont faites des nouvelles technologies, en particulier lorsque ces utilisations visent une extension des champs et de l'intensité des contrôles.
La première partie du livre aborde la question de la technologie digitale et du contrôle comme une ressource colossale d'informations sur les individus et leurs comportements convoitée pour leur valeur tant commerciale que sécuritaire. Elle fait également le point sur les technologies utilisées dans cette chasse à l'info : puces-RFID, caméras d'observation, navigateurs du web, scanners, kits-ADN, spywares, banques de données avec programmes algorithmiques, satellites d'écoute, bodyscans, etc. Les effets secondaires de ce développement sont aussi clairs que pervers clairs : une perte non seulement de confidentialité mais également une perte de «soi». Gouvernements, entreprises, agences publicitaires ne sont plus transparents mais le citoyen, quant à lui, le devient complètement... et sans consentement!
La guerre contre le terrorisme fait l'objet d'une analyse dans la seconde partie de l'ouvrage.
L'accent est, enfin, mis sur la montée en puissance de l'Union Européenne en tant qu'institution de contrôle. L'auteur fait le constat que, à travers sa structure de sécurité complexe et non contrôlée, la rhétorique de l'Union sur les droits de l'Homme se situe souvent en totale contradiction avec sa pratique ; les droits humains devenant pour une contrainte, voire un obstacle au contrôle social.
Cet ouvrage très accessible offre des clés de lecture et des perspectives pertinentes quant à la place et au rôle des nouvelles technologies dans notre siècle au regard des libertés fondamentales.

Jean-Pierre Borloo, Journaliste indépendant

Le journaliste n'est pas (toujours) un voyeur

La presse est de plus en plus souvent pointée du doigt s'agissant de ses intrusions dans la vie privée des citoyens et des hommes publics. Cette… mauvaise presse des médias est-elle justifiée et quelles sont les limites à ne pas franchir en la matière ?

La presse exagère, elle s'insinue toujours plus dans la vie privée des gens, s'en empare pour en livrer tous les détails tel un charognard. De telles affirmations fusent sur les réseaux sociaux et dans les forums. Certains juristes vont plus loin encore, en demandant même que l'on restreigne la liberté de la presse pour cette raison précise[1]. Allons, allons… S'en prendre à un principe constitutionnel parce que certains médias dépassent parfois les limites est totalement exagéré. Comme si on limitait les libertés des avocats parce que certains ne défendent pas correctement leurs clients ou que l'on remette en cause l'indépendance de la magistrature en raison de mauvais jugements rendus…

Ce genre d'exagération est une caricature. La réalité est bien plus nuancée. La presse ne fait pas n'importe quoi même si l'on constate une «peopolisation» croissante de l'information. Une partie de la presse a toujours été friande de faits divers où l'on est inévitablement amenés à franchir la porte de la sphère privée. En Belgique moins qu'en Grande Bretagne ou qu'en France où s'égaient des journaux à sensation que nous n'avons pas chez nous. Alors, rien de neuf ? Rien à déclarer sur le terrain de violation de la vie privée ?

Dérives et (auto-)régulation Si bien sûr. La «peopolisation» a rattrapé tous les médias, même ceux dits sérieux. Tous se délectent d'émotions, de vécu, d'humain même quand l'apport informatif est faible. C'est peut-être une conséquence de l'affaire Dutroux. 300.000 personnes clamaient, dans la rue, que la justice devait être plus humaine, moins froide, plus à l'écoute des sentiments des gens. La presse, en pleine perte d'audience, l'a pris pour elle. Et elle colle désormais de l'émotion et de l'humain sur tous les sujets. De préférence, vu la concurrence, le plus rapidement possible. Le temps de l'information est devenu l'immédiateté. Raison de plus pour faire dans l'émotionnel plutôt que dans l'analyse.

Les personnes s'exposent elles-mêmes de plus en plus sur les réseaux sociaux. Tout y est livré, en détails et en images. Les personnalités publiques divulguent elles-mêmes, toujours davantage, leur vie privée en public. Les médias ne sont pas les seuls responsables de l'intrusion dans la sphère privée.

Ce contexte nouveau pousse-t-il davantage à la faute ? Possible. La profession toute entière ne s'est cependant pas croisée les bras. Elle a mis en place un système d'autorégulation. Le Conseil de déontologie journalistique (CDJ) fonctionne depuis 2009, avec des représentants des médias mais aussi de la société civile. Il a pour mission d'affiner la déontologie des journalistes (un nouveau code a été adopté en 2013), de traiter les plaintes qui visent des médias ou des journalistes, et d'informer le public et les intéressés sur les règles de bonne conduite éditoriale.

Son activité est intense. En 2015, devrait notamment être finalisé un avis contraignant sur la manière de permettre, ou non, l'identification des personnes dans les médias. Le non respect de la vie privée est un problème. Il fait partie du trio de tête des plaintes adressées au CDJ. Mais l'organe d'autorégulation s'en occupe. Sinon, les poursuites civiles contre des journalistes peuvent également avoir lieu. Et il y en a !

Vie privée vs. Intérêt sociétal Que dit la déontologie journalistique ? Globalement, qu'il faut respecter la vie privée. Mais que dans certains cas l'intrusion dans cette sphère est justifiée, s'il en va de l'intérêt public (et non du public, ce n'est pas la même chose), autrement dit de l'intérêt sociétal. Cela vaut pour toutes les personnes, même si la sphère privée inviolable est plus réduite chez les personnalités publiques.

La loi interdit aussi certaines diffusions d'informations privées. Notamment en ce qui concerne des mineurs d'âge impliqués dans des affaires judiciaires ou de mœurs.

Donc, dire que la situation est déplorable, que les journalistes bafouent tous les droits au nom de la liberté de l'information est complètement exagéré. Des recours existent, en cas de violation présumée de droits. Aux personnes qui se sentent atteintes dans leur intégrité de les actionner.

(1) L'avocat Jean-Marie Dermagne et le juge à la retraite Christian Panier signaient une carte blanche dans La libre Belgique, le 18 novembre 2014, disant que, dans certaines circonstances, «les médias devraient être forcés au silence».

État des droits de l'Homme en Belgique

RAPPORT 2014-2015

Un dossier réalisé par la Ligue des droits de l'Homme

Sommaire

La Ligue dans votre quotidien

Vous souhaitez vous investir dans une section locale de la Ligue des droits de l'Homme ? La LDH est aussi près de chez vous ! Vous souhaitez mettre sur pied une section locale LDH ou une/des activités visant à soutenir notre association : contactez le secrétariat de la LDH au 02 209 62 80 – ldh@liguedh.be

Charleroi	Jacques PRIME		prime.jacques@brutele.be
La Louvière	Marie-Louise ORUBA	064/22 85 34	mloruba@hotmail.com
Louvain-la-Neuve	KAP droits de l'Homme Passage des Dinandiers, 1/208 1348 Louvain-la-Neuve		kapdroitsdelhomme@kapuclouvain.be
Mons	Karim ITANI		k.itani@avocat.be
Namur	Henry BRASSEUR		h_brasseur@yahoo.fr
Verviers	Jeannine CHAINEUX Rue Michel Pire, 17 4821 Andrimont	0474/750 674	jeanine.chaineux@cgsp.be

LA LDH SUR LE WEB 2.0

Groupes Facebook : «Ligue des droits de l'Homme» et «des droits qui craquent»
Ce groupe poursuit un objectif d'information sur les enjeux des nouvelles technologies en matière de vie privée. Il tient également informé ses membres des activités de la LDH.
Suivre la LDH sur Twitter :
@liguedh_be
#droitsquicraquent
#toutlemondetoutnu
Suivez l'actualité de la LDH sur votre mobile et diffusez la.




Aidez-nous à défendre vos droits fondamentaux !

La Ligue des droits de l'Homme est une association indépendante. Elle ne peut survivre sans l'apport financier des citoyens qui souhaitent qu'elle continue son combat au quotidien pour la défense des droits fondamentaux en Belgique. Vous pouvez nous soutenir concrètement.

➔ A partir de 65€ (52,50€ étudiants, chômeurs, minimexés, pensionnés), vous devenez **membre donateur**. Vous recevez la carte de membre (réduction dans certains cinémas, théâtres...) et une déduction fiscale.

➔ A partir de 25€ (12,5 € étudiants, chômeurs, minimexés, pensionnés), vous devenez **membre**. Vous recevrez la carte de membre et profitez des avantages exclusifs membres réservés aux membres.

➔ A partir de 40€, vous devenez **donateur** et profitez d'une déduction fiscale.



La Ligue des droits de l'Homme adhère au Code éthique de l'AERF. Vous avez un droit à l'information. Ceci implique que les donateurs, collaborateurs et employés sont informés au moins annuellement de l'utilisation des fonds récoltés. Le rapport d'activité et le bilan financier de la LDH pour l'année 2013 sont consultables sur www.liguedh.be

Ligue des droits de l'Homme asbl · Rue du Boulet 22 à 1000 Bruxelles
Tél. : 02 209 62 80 · Fax : 02 209 63 80 · Courriel : ldh@liguedh.be · Web : www.liguedh.be

Vous aussi, rejoignez notre mouvement !

❏ Je souhaite devenir **membre donateur** et je verse .... (à partir de 65€/52,50€)
❏ Je souhaite devenir **membre** et je verse .... (à partir de 25€/12.5€)
❏ Je souhaite devenir **donateur** et je verse .... (déductible à partir de 40€)

sur le compte de la Ligue des droits de l'Homme : CP 000-0000182-85

Facilitez-vous la vie : versez via un ordre permanent (OP) !
Pour ce faire, divisez votre montant par 12 et contactez votre organisme bancaire pour la procédure.

❏ Je verse le montant via un ordre permanent
❏ Vous pouvez également vous rendre sur **www.liguedh.be** et effectuer un paiement en ligne à l'aide de votre carte de crédit

PayPal™

Nom : .... Prénom : ....
Adresse : ....
Année de naissance : .... Profession : ....
Tél : .... Courriel : ....
Signature : ....



La Ligue des droits de l'Homme asbl

présente

TOUT LE MONDE TOUT NU









POINTCULTURE



De janvier à décembre 2015

À BRUXELLES ET EN WALLONIE

Du 9 au 11 octobre 2015

AU CENTRE CULTUREL JACQUES FRANCK (ST-GILLES)

Programme : ***www.liguedh.be/72430***



Groupe FB : « Des droits qui craquent »



@liguedh_be #toutlemondetoutnu #droitsquicraquent